UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

DOUGLAS NEWELL, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CITRIX SYSTEMS, INC., a corporation,
FIDELITY NATIONAL FINANCIAL, INC., a corporation, and
LOANCARE, LLC, a corporation

Defendants.

Case No.:

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Douglas Newell, individually and on behalf of the Class defined below of similarly situated persons, allege the following against Citrix Systems, Inc. ("Citrix"), Fidelity National Financial, Inc. ("FNF"), and LoanCare, LLC ("LoanCare") (collectively "Defendants") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

SUMMARY OF THE CASE

1. This case involves a critical flaw in Defendant Citrix's NetScaler software, which allowed hackers and other bad actors to obtain individuals' PII for unsavory and illegal purposes. Specifically, the flaw resulted in the Data Breach that Defendant LoanCare, LLC announced on December 12, 2023, wherein—on November 19, 2023—the personal identifying information ("PII") of millions of individuals was exposed to unauthorized third parties.

2. About 1.31 million individuals' PII was compromised from the Data Breach.

3. This Class Action Complaint is filed on behalf of all persons in the United States, described more fully in the following sections, whose PII was compromised in the Data Breach.

JURISDICTION AND VENUE

4. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

5. This Court has jurisdiction over Defendants because they have availed themselves of the rights and benefits of the State of Florida by engaging in activities including (i) directly and/or through their parent companies, affiliates and/or agents providing services throughout the United States in this judicial district and abroad; (ii) conducting substantial business in this forum; (iii) having a registered agent to accept service of process in the State of Florida; and/or (iv) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in Florida and in this judicial District.

6. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) because Defendant Citrix resides within this District, and because Defendants purposefully engaged in activities, including transacting business in this District and engaging in the acts and omissions alleged herein, in this District.

PARTIES

A. Plaintiff Douglas Newell

7. Plaintiff Douglas Newell is, and at all relevant times alleged herein was, an individual citizen of the State of Louisiana.

8. Plaintiff is a LoanCare customer who received a loan from LoanCare.

9. On January 3, 2024, Plaintiff received a Notice of Data Breach from LoanCare, saying that Plaintiff's PII was compromised, including, *inter alia*, his name, address, Social Security Number ("SSN"), and Loan Number.

10. Upon learning of the Data Breach, Plaintiff spent time planning how to protect his personal information.

11. In addition to the damages detailed herein, the Data Breach has caused Plaintiff to be at substantial risk for further identity theft and fraud using his stolen PII.

B. LoanCare, LLC

12. Defendant LoanCare is a mortgage servicer operating in the United States.

13. LoanCare is headquartered in NMLS# 2916, 3637 Sentara Way, Virginia Beach, Virginia 23452.

C. Fidelity National Financial, Inc. ("FNF")

14. Defendant FNF is a provider of title insurance and settlement services to real estate and mortgage industries.

15. FNF claims to be "#1 in market share in the residential purchase, refinance, and commercial markets . . . ."[1]

16. FNF is headquartered in 601 Riverside Avenue, Building 5, Jacksonville, Florida 32204.

17. FNF is the parent company of Defendant LoanCare, LLC.[2]

D. Citrix Systems, Inc.

[1] ***FNF Home Page***, Fidelity National Financial, Inc., https://fnf.com/.
[2] ***Fidelity National Financial, Inc. Announces Acquisition of LoanCare Servicing Center, Inc***., Fidelity National Financial, Inc., https://www.investor.fnf.com/news-releases/news-release-details/fidelity-national-financial-inc-announces-acquistion-loancare/.

18. Defendant Citrix is incorporated in the State of Florida, with its corporate office located at 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States.

19. On or about September 2022, Vista Equity Partners and Elliot Investment Management, L.P. acquired Citrix and combined Citrix with TIBCO Software ("TIBCO").[3]

20. Both Citrix and TIBCO are subsidiaries of their parent company, the Cloud Software Group.[4]

21. Defendant is a cloud computing and virtualization company which provides server, application, and desktop virtualization, networking, software as a service ("SaaS"), and cloud computing products.

22. Defendant Citrix "serves more than 100 million users, 10,000 partners and 400,000 customers across 100 countries."[5]

23. Defendant Citrix collects and stores PII of its users for providing its services.

FACTUAL ALLEGATIONS

A. NetScaler Generally

24. NetScaler is a suite of software products designed to facilitate, manage, and protect network traffic.[6]

25. The NetScaler brand, like Citrix, is included under the Cloud Software Group name.[7]

---

[3] *Vista Equity Partners and Evergreen Coast Capital Announce the Completion of the Transaction to Acquire Citrix Systems and Combine it with TIBCO Software*, Cloud Software Group, https://www.cloud.com/news/press-release.
[4] *Mission-critical enterprise software at scale*, Cloud Software Group, https://www.cloud.com/.
[5] *Data Index,* Citrix, https://www.citrix.com/about/sustainability/2021-report/data-index.html#:~:text=Citrix%20serves%20more%20than%20100,400%2C000%20customers%20across%20100%20countries (last visited Dec. 26, 2023).
[6] *Citrix NetScaler: What Is It? | Parallels Insights*, Parallels, https://www.parallels.com/blogs/ras/citrix-netscaler/.
[7] *Vista Equity Partners and Evergreen Coast Capital Announce the Completion of the Transaction to Acquire Citrix Systems and Combine it with TIBCO Software*, Cloud Software Group, *supra*.

26. To use NetScaler, a piece of hardware hosting the different NetScaler products ("NetScaler appliance") is necessary.[8] After obtaining and unpacking the NetScaler appliance, the NetScaler appliance must be configured.[9]

27. Of the configurations recommended in the NetScaler product documentation are controls for authentication, authorization, and auditing ("AAA"):

a. **Authentication**—NetScaler verifies a client's credentials and approves or denies to that client access to protected servers.

b. **Authorization**—NetScaler determines which content on a protected server a client can access.

c. **Auditing**—NetScaler keeps a record of each client's activity on a protected server.[10]

28. Two of NetScaler's software product are relevant here: (a) NetScaler Application Delivery Controller ("ADC") and (b) NetScaler Gateway.

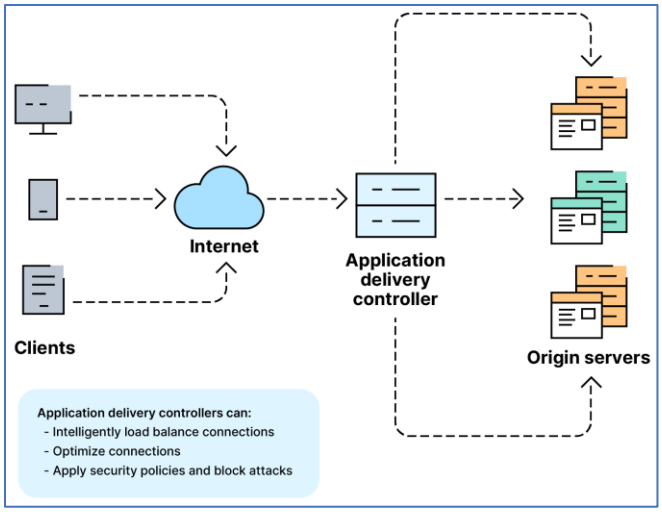
a. NetScaler Application Delivery Controller

29. An application delivery controller ("ADC") is "purpose-built networking appliance used to improve the performance, security, and resiliency of applications delivered over the web."[11]

30. ADCs can efficiently load balance connections between devices, optimize such connections, apply security policies, and block attacks.[12]

---

[8] *Install the hardware*, NetScaler Product Documentation, https://docs.netscaler.com/en-us/citrix-adc/current-release/getting-started-with-citrix-adc/install-hardware.
[9] *Id.*
[10] *How authentication, authorization, and auditing works*, NetScaler Product Documentation, https://docs.netscaler.com/en-us/citrix-adc/current-release/aaa-tm/how-citrix-adc-aaa-works.
[11] *What is an application delivery controller?*, NetScaler, https://www.netscaler.com/articles/what-is-an-application-delivery-controller.
[12] *Id.*

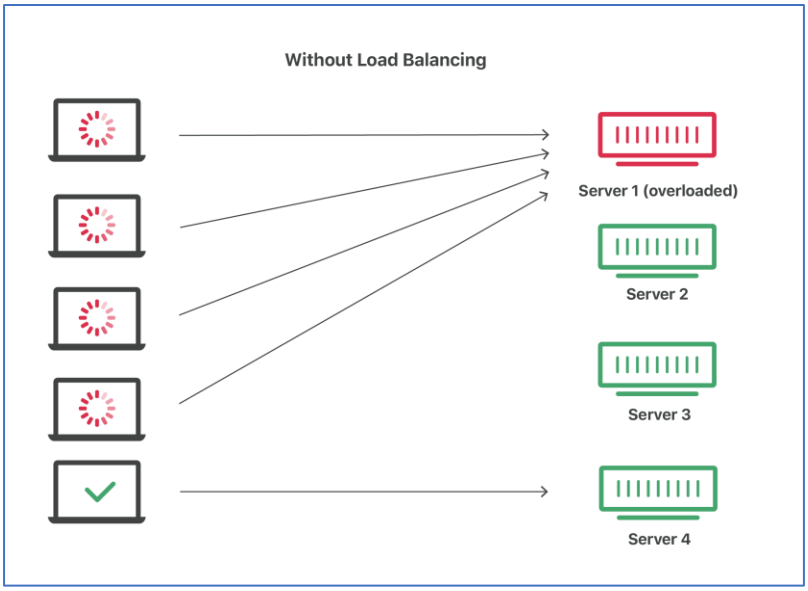


31. 'Load balancing' is the distribution of network traffic among several servers to ameliorate a service or application's performance and soundness.[13]

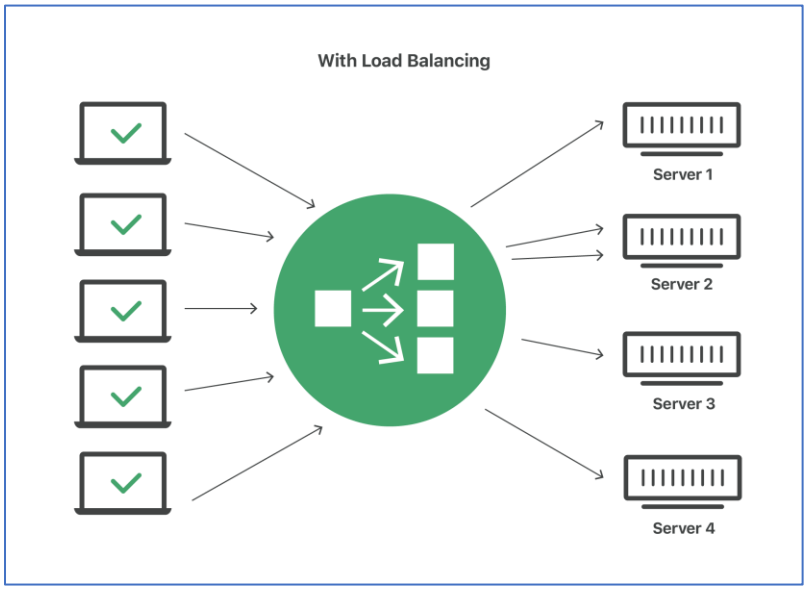
32. A 'server' is a device or computer program that delivers a service to a 'client', another computer program or device.[14] Examples of services include, *inter alia,* accessing databases, using e-mail, providing files, and deploying websites.[15]

33. Under the 'client-server' model, the client sends over the network a service request to the server, and the server responds to the client, the response of which may allow or deny the client access to the desired service.

[13] *What is load balancing? | How load balancers work,* CloudFlare, https://www.cloudflare.com/learning/performance/what-is-load-balancing/.
[14] *What is a Server?*, GeeksforGeeks, https://www.geeksforgeeks.org/what-is-server/.
[15] *Id.*



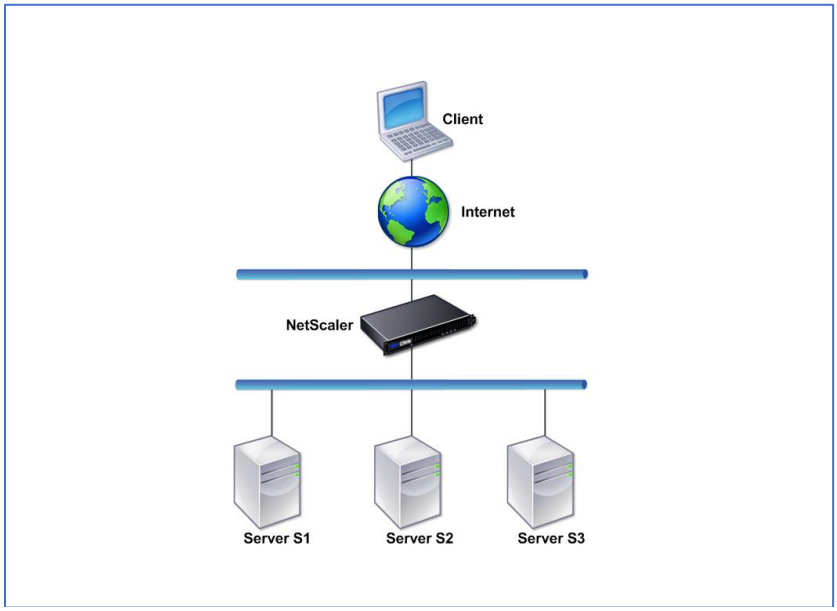
34. Load balancing removes strain on servers, making them more efficient, improving performance and reducing the amount of time it takes for a piece of data to go from one place to another.[16]



b. NetScaler Gateway

[16] *What is load balancing? | How load balancers work*, CloudFlare, *supra*.

35. Information technology practitioners of a company use NetScaler Gateway by placing it on the company's internal network as "a secure single point of access to the servers, applications, and other network resources that reside in the internal network."[17]



The black device is the 'NetScaler appliance', which hosts the different NetScaler software products (e.g., NetScaler ADC, NetScaler Gateway).

36. A 'gateway' is a network node "that connects two networks with different transmission protocols together."[18]

37. A 'network' compromises two or more devices (e.g., computers, tablets, gaming consoles) that are connected to share resources, exchange files, or permit electronic communication.[19]

38. A 'network node' is a point of connection among network devices that can obtain and deliver data from one endpoint (i.e., a physical device connected to a network) to the other.[20]

[17] *Common NetScaler Gateway Deployments*, NetScaler Gateway Product Documentation, https://docs.netscaler.com/en-us/citrix-gateway/current-release/common-gateway-deployments.
[18] *Definition (gateway)*, TechTarget, https://www.techtarget.com/iotagenda/definition/gateway.
[19] *What is a Network?*, Fla. Cent. For Instructional Tech., https://fcit.usf.edu/network/chap1/chap1.htm.
[20] *What is a Network Node?*, SolarWinds, https://www.solarwinds.com/resources/it-glossary/network-node.

39. A 'protocol' is "established set of rules that determine how data is transmitted between different devices in the same network[,]" the rules of which permit network-connected devices to communicate with each other.[21]

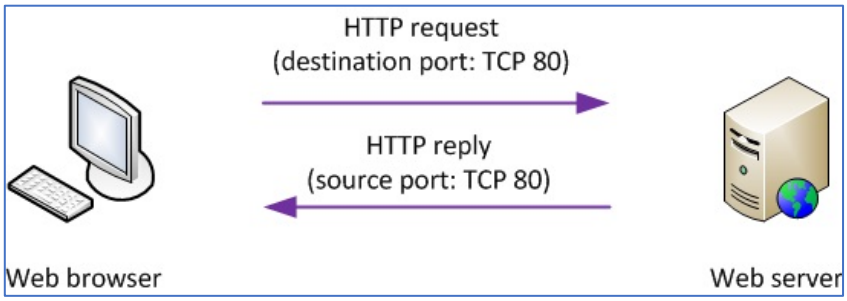
40. Many protocols are associated with certain 'ports', which are virtual points where network connections start and finish. Each port is affiliated with a particular service; accordingly, for way of example, emails are sent to one port, and web pages go to another port.[22]

41. Each port has an assigned 'port number'. While there are 65,535 potential port numbers, popular port numbers include, *inter alia*:

a. **Port 22** for **Secure Shell**, which allows for creation of secure network connections;

b. **Port 123** for **Network Time Protocol**, which permits computer clocks to synchronize with each other; and

c. **Port 80** for **Hypertext Transfer Protocol**, which allows for delivery and receipt of unencrypted web traffic.[23]



c. "Citrix Bleed" Vulnerability (CVE-2023-4966)

[21] *What is a Network Protocol, and How Does It Work?*, CompTIA, https://www.comptia.org/content/guides/what-is-a-network-protocol.
[22] *What is a computer port | Ports in networking*, CloudFlare, https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/.
[23] *Id.*

42. On October 10, 2023, Citrix announced a sensitive information disclosure vulnerability in its NetScaler software suite. The NetScaler vulnerability is known as "Citrix Bleed."[24]

43. Citrix Bleed allows hackers to hijack user sessions on NetScaler appliances to gather configuration information about the target company's network and steal credentials from the target company.[25]

44. To exploit Citrix Bleed, an attacker sends certain web traffic to a NetScaler appliance, which will cause the NetScaler appliance to return contents of system memory. Such memory contents can include an AAA session cookie. With the session cookie, which is a piece of data containing an identifier associated with a validated NetScaler user,[26] the attacker can bypass ordinary authentication procedures (i.e., username, password, multi-factor authentication) and interact with the NetScaler appliance.[27]

45. On October 10, 2023, Citrix released a patch to fix the Citrix Bleed Vulnerability. Additional mitigation steps were released on October 23.[28]

46. Citrix Bleed was being exploited as a zero-day vulnerability since at least August 2023.[29]

---

[24] ***Notice to Customers of Data Security Incident***, Xfinity, https://assets.xfinity.com/assets/dotcom/learn/_Data_Incident.pdf; ***Comcast's Xfinity breached by Citrix Bleed; 36 million customer's data accessed***, Malwarebytes Labs, https://www.malwarebytes.com/blog/news/2023/12/comcasts-xfinity-breached-by-citrix-bleed-36-million-customers-data-accessed.

[25] ***Comcast bleeds 36M credentials in Citrix-related breach***, Fierce Telecom, https://www.fiercetelecom.com/telecom/xfinity-reports-breach-affecting-358m-customer-ids#:~:text=The%20data%20breach%20was%20discovered,a%20notice%20from%20the%20company.

[26] ***See What are cookies?***, Kapersky Lab, https://usa.kaspersky.com/resource-center/definitions/cookies.

[27] ***Investigation of Session Hijacking via Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966)***, Mandiant, https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966.

[28] ***Notice to Customers of Data Security Incident; see also NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967***, Citrix, https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967.

[29] **Remediation for Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966)**, Mandiant, https://www.mandiant.com/resources/blog/remediation-netscaler-adc-gateway-cve-2023-4966.

B. LoanCare Data Breach

47. On November 19, 2023, Defendant FNF, LoanCare's parent company, filed a Form 8-K Report notifying the Securities and Exchange Commission ("SEC") the following about the Data Breach:

> Fidelity National Financial, Inc. ("FNF" or the "Company") recently became aware of a cybersecurity incident that impacted certain FNF systems. FNF promptly commenced an investigation, retained leading experts to assist the Company, notified law enforcement authorities, and implemented certain measures to assess and contain the incident. Among other containment measures, we blocked access to certain of our systems, which resulted in disruptions to our business. For example, the services we provide related to title insurance, escrow and other title-related services, mortgage transaction services, and technology to the real estate and mortgage industries, have been affected by these measures. Our majority-owned subsidiary, F&G Annuities & Life, a leading provider of insurance solutions, was not impacted by the incident.
>
> Based on our investigation to date, FNF has determined that an unauthorized third party accessed certain FNF systems and acquired certain credentials. The investigation remains ongoing at this time.
>
> FNF will continue to assess the impact of the incident and whether the incident may have a material impact on the Company.
>
> We are working diligently to address the incident and to restore normal operations as quickly and safely as possible.[30]

48. On December 12, 2023, Defendant LoanCare posted its Notice of Data Event on the Maine Attorney General's website, notifying the public for the first time of the Data Breach, in which LoanCare specified the following:

> **What Happened?**
> On or about November 19, 2023, LoanCare, LLC ("LoanCare"), which performs or has performed loan subservicing functions for your mortgage loan servicer, became aware of unauthorized access to certain systems within its parent's, Fidelity National Financial, Inc. ("FNF"), information technology network. Upon becoming aware of the incident, FNF commenced an investigation with the assistance of third-party experts, notified certain law enforcement and governmental authorities, and

[30] ***Fidelity Nat'l Finan., Inc.,*** 8-K Report (Form 8-K) (Nov. 19, 2023).

> began taking measures to assess and contain the incident. The incident has been contained.
>
> The investigation has determined that an unauthorized third party exfiltrated data from certain FNF systems. As part of the review of the potentially impacted data, LoanCare identified that some of your personal information may have been among that data. It is important to note that we have not identified any fraudulent use of your personal information as a result of this incident.
>
> **What Information Was Involved?**
> Based on our investigation, we understand that your Name, Address, Social Security Number, and Loan Number may have been obtained by the unauthorized third party.

49. The compromised information included names, addresses, Social Security Numbers, and loan numbers.

50. In the Notice of Data Breach, LoanCare advised consumers to monitor accounts, obtain freeze credits and/or new credit reports, report identity theft to the Federal Trade Commission ("FTC") and police, and issue fraud alerts.

51. The PII of about 1,316,938 individuals was affected by the Data Breach.[31]

52. Upon information and belief, the Data Breach was caused by an unknown and unnamed attacker exploiting the "Citrix Bleed" vulnerability in NetScaler appliances affiliated with Defendant FNF's domain (i.e, fnf.com).[32]

53. A domain is an address used to enter websites (e.g., google.com, yahoo.com).[33]

54. After Kevin Beaumont, a cybersecurity researcher, performed Shodan[34] scans of NetScaler appliances linked to FNF's domain, Mr. Beaumont deduced that FNF applied the

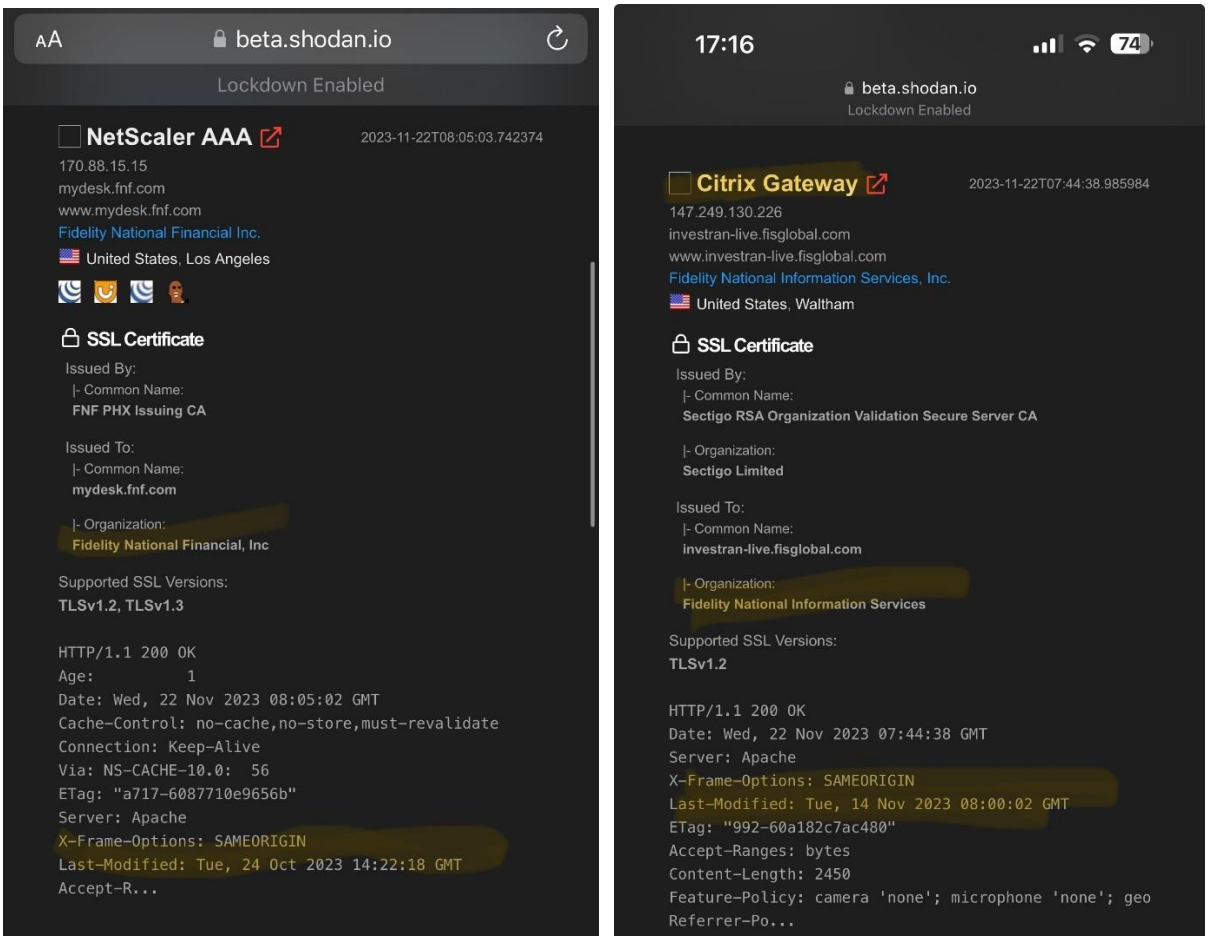
---

[31] *Id*.
[32] ***BlackCat claims it is behind Fidelity National Financial ransomware shakedown***, The Register, https://www.theregister.com/2023/11/23/blackcat_ransomware_fnf/.
[33] **What is a domain name? | Domain name vs. URL,** CloudFlare, https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/.
[34] Shodan is a search engine that permits users to search for information about Internet of Things ("IoT") devices, such as power plants, mobile phones, refrigerators, etc. ***See*** **Shodan Home Page**, Shodan, https://www.shodan.io/.

patch two weeks after it was made available (i.e., FNF applied the patch on or about November 14, 2023).[35]

55. Mr. Beaumont noted that FNF "patched []Citrix Bleed late and now [has] security incident involving a ransomware group."[36]

56. Upon information and belief, the Cyber Attack on FNF's systems was perpetrated by the ransomware gang, AlphV/Black Cat.[37]



Results of Kevin Beaumont's Shodan scans of NetScaler appliances linked to FNF's domain.

C. Defendants Failed to Comply with the FTC Act and Failed to Observe Reasonable and Adequate Date Security Measures

[35] **Kevin Beaumont (@GossiTheDog@cyberplace.social)**, Mastodon (Nov. 22, 2023, 3:39PM), @https://cyberplace.social/@GossiTheDog/111456129025977120.
[36] Id.
[37] **Notorious ransomware gang takes credit for cyberattack on Fidelity National Financial**, The Record, https://therecord.media/fidelity-national-financial-ransomware-alphv-black-cat.

57. The FTC has issued several guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be considered for all business decision-making.[38]

58. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[39]

59. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

60. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[40]

61. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

---

[38] *Start With Security*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[39] *Protecting Personal Information: A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[40] *Start With Security*, *supra*.

Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

62. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

63. Plaintiff and Class Members gave their PII to Defendants LoanCare and FNF with the reasonable expectation and understanding that Defendants' third-party vendors, like Defendant Citrix, would comply with their duty to keep such information confidential and secure from unauthorized access.

64. The Cloud Software Group stated in its Data Processing Addendum the following about the Security of personal data processed by the Cloud Software Group:

> *We shall implement and maintain appropriate administrative, technical, and organizational practices designed to protect Personal Data against any misuse or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data*. Such security practices are set forth in the Cloud SG Security Exhibit, which is available at https://www.cloud.com/trust-center/citrix-services-security-exhibit. We seek to continually strengthen and improve its security practices, and so reserve the right to modify the controls described herein. Any modifications will not diminish the level of security during the relevant term of Products and/or Services.
>
> Our employees are bound by appropriate confidentiality agreements and required to take regular data protection training as well as comply with Our corporate privacy and security policies and procedures.[41]

65. The Cloud Software Group's Data Processing Addendum states that the Addendum "**applies to the Processing of Personal Data by Cloud Software Group, Inc. and <u>its Affiliates</u>**

[41] *Data Processing Addendum*, Cloud Software Group, https://www.cloud.com/content/dam/cloud/documents/legal/cloud-software-group-data-processing-addendum-oct-2023.pdf.

on Your behalf when providing Cloud SG products ("Products") and technical support services or consulting services ("Services")."[42]

66. Regarding Plaintiff's and Class Members' Private Information, Defendant FNF states the following in its Financial Privacy Notice:

> Fidelity National Financial, Inc. and its majority-owned subsidiary companies (collectively, "FNF," "our," or "we") respect and are committed to protecting your privacy.
> …
>
> A limited number of FNF subsidiaries have their own privacy notices. *If a subsidiary has its own privacy notice, the privacy notice will be available on the subsidiary's website and this Privacy Notice does not apply*.
> …
>
> **Security of Your Information**
> We maintain physical, electronic, and procedural safeguards to protect your Personal Information. [43]

67. Defendant LoanCare posts the following in its own Privacy Notice regarding Plaintiff's and Class Members' Private Information:

> Fidelity National Financial, Inc. and its majority-owned subsidiary companies (collectively, "FNF," "our," or "we") respect and are committed to protecting your privacy.
> …
>
> **Security of Your Information**
> We maintain physical, electronic, and procedural safeguards to protect your Personal Information.[44]

68. Defendants have been on notice for years that Plaintiff's and Class Members' PII was a target for bad actors because of, among other motives, the high value of the PII created, collected and maintained by Defendants.

---

[42] *Id.*
[43] **Fidelity Nat'l Finan. Privacy Not.**, Fidelity Nat'l Finan., Inc., https://fnf.com/privacy-notice.
[44] **Fidelity Nat'l Finan. Privacy Not**., LoanCare, LLC, https://www.loancareservicing.com/privacy-policy/.

69. Despite such awareness, Defendants failed to impose and maintain reasonable and appropriate data security controls to protect Plaintiff's and Class Members' PII from unauthorized access that Defendants should have anticipated and guarded against.

70. Defendants were fully aware of their obligation to protect the PII of their customers and users because of their collection, storage, and maintenance of PII. Defendants were also aware of the significant consequences if they failed to do so because they collected, stored, and maintained sensitive private information from millions of individuals, and Defendants knew that this information, if hacked, would result in injury to consumers, including Plaintiff and Class Members.

71. Despite understanding the consequences of insufficient data security, Defendants failed to adequately protect Plaintiff's and Class Members' PII, permitting bad actors to access and misuse it.

D. Defendants Failed to Comply With Industry Standards

72. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks.[45] All organizations collecting and handling PII, such as Defendants, are strongly encouraged to follow these controls.

73. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any

[45] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), available at https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf.

governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[46]

74. Several best practices have been identified that a minimum should be implemented by companies like Defendants, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[47]

75. Defendants failed to follow these and other industry standards to adequately protect the PII of Plaintiff and Class Members.

E. The Data Breach Caused Harm and Will Result in Additional Fraud

76. Without detailed disclosure to the victims of the Data Breach, individuals whose PII was used and maintained by Defendants, including Plaintiff and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of their PII for months without being able to take precautions to prevent imminent harm.

77. The ramifications of Defendants' failure to secure Plaintiff's and Class Members' data are severe.

78. Consumer victims of data breaches are much more likely to become victim of identity fraud. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.[48]

[46] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Jan. 5, 2021).
[47] *See* Center for Internet Security, *Critical Security Controls*, *supra*.
[48] *2014 LexisNexis True Cost of Fraud Study*, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf, (last visited July 26, 2018).

79. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[49] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[50]

80. Identity thieves can use PII, such as that of Plaintiff and Class Members, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

81. As a result of Defendant LoanCare's delay between their knowledge of the Data Breach and the notice of the Data Breach sent to affected persons in December 12, 2023, the risk of fraud for Plaintiff and Class Members has been driven even higher.

82. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[51]

83. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending

[49] 17 C.F.R § 248.201 (2013).
[50] Id.
[51] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 10, 2017).

an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[52]

84. There may be a time lag between when harm occurs versus when it is discovered, and also between when private information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[53]

85. Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

F. Plaintiff and Class Members Suffered Damages

a. **Plaintiff Newell's Damages**

86. Following the Data Breach, Plaintiff Newell noticed an increase in spam emails, text messages, and/or phone calls.

87. As a result of the Data Breach, Mr. Newell has had to pay for credit monitoring, identify theft prevention, and/or a credit card security plan.

88. Mr. Newell has spent time and effort dealing with and mitigating the consequences of the Data Breach.

89. Mr. Newell has spent about two (2) hours searching for fraudulent charges on his accounts and a total of about four (4) hours in dealing with the consequences of the Data Breach.

---

[52] *Victims of Identity Theft*, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 10, 2017).
[53] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

90. From the Data Breach, Mr. Newell has and continues to suffer emotional distress, for he has trouble sleeping from researching developments on the Data Breach and protecting his accounts from potential fraud.

b. The Nationwide Class

91. The Data Breach was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

92. Had Defendant Citrix remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant Citrix would have prevented intrusion into its information storage and security systems and, ultimately, the theft of the PII of over 1.31 million individuals.

93. As a direct and proximate result of Defendants' wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing

and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

94. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their PII;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market; and,

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience,

nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

95. While Plaintiff's and Class Members' private information have been stolen, Defendants continue to hold individuals' PII, including Plaintiff's and Class Members'. Particularly because Defendants have demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their private information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ALLEGATIONS

96. Plaintiff brings this Action as a class action under Federal Rule of Civil Procedure 23 and seeks certification of the following nationwide Class ("Class"):

> All persons whose personal information was accessed, compromised, copied, stolen, and/or revealed as a result of Defendants' (and any of Defendants' affiliates and customers) Data Breach.

97. Excluded from the Class are Defendants, their officers and directors, and Members of their immediate families or their legal representatives, heirs, successors or assigns and any entity in which Defendants have or had a controlling interest.

98. Class certification of Plaintiff's claims is appropriate because **he** can prove the elements of the claims on a class-wide basis utilizing the same evidence as would be used to prove those elements in separate actions alleging the same claims.

99. **Numerosity—Federal Rule of Civil Procedure 23(a)(1)**. The Members of the Class are so numerous that joinder of all Class Members would be impracticable. Upon information and belief, the Class numbers in the millions. Also, the Class is comprised of an easily ascertainable set of individuals who were impacted by the Data Breach. The exact number of Class

Members can be confirmed through discovery, which includes Defendants' records. The resolution of Plaintiff's and Class Members' claims through a class action will behoove the Parties and this Court.

100. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3)**. Common questions of fact and law exist as to all Members of the Class and predominate over questions affecting only individual Class Members. These common questions of law or fact, include, among other things:

- Whether Defendants' cybersecurity systems and/or protocols before and during the Data Breach complied with relevant data security laws and industry standards;
- Whether Defendants properly implemented their purported security measures to safeguard Plaintiff's and Class Members' private information from unauthorized access, propagation, and misuse;
- Whether Defendants took reasonable measures to determine the extent of the Data Breach after they first discovered the same;
- Whether Defendants disclosed Plaintiff's and Class Members' private information in contravention of the understanding that the information was being revealed in confidence and should be maintained;
- Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures and security controls to preclude unauthorized access to Plaintiff's and the Class Members' private information;
- Whether Defendants were unjustly enriched by their actions; and
- Whether Plaintiff and Class Members are entitled to damages, injunctive relief, or other equitable relief, and the extent of such damages and relief.

101. Defendants engaged in a common course of conduct granting rise to the legal rights sought to be enforced by Plaintiff, on behalf of themselves and other Members of the Class. Similar or identical common law violations, business practices, and injuries are involved.

102. **Typicality—Federal Rule of Civil Procedure 23(a)(3)**. Plaintiff's claims are typical of the claims of the other Members of the Class because, *inter alia*, all Class Members were similarly injured and sustained similar monetary and economic injuries as a result of Defendants' misconduct described herein and were accordingly subject to the alleged Data Breach. Also, there are no defenses available to Defendants that are unique to Plaintiff.

103. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4)**. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class he seeks to represent, he retained counsel competent and experienced in complex class action litigation, and he will prosecute this action earnestly. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

104. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2)**. Defendants acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate regarding the Class under Federal Rule of Civil Procedure 23(b)(2).

105. **Superiority—Federal Rule of Civil Procedure 23(b)(3)**. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class Members to individually seek redress for Defendants' wrongful conduct. Even if Class

Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

106. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

- The prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications establishing conflicting standards of conduct for Defendants;

- The prosecution of separate actions by individual Class Members would create a risk of adjudication that would be dispositive of the interests of other Class Members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests; and

- Defendants have acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief regarding the Members of the Class as a whole.

107. Class certification is also appropriate because this Court can designate specific claims or issues or class-wise treatment and may designate multiple subclasses under Federal Rule of Civil Procedure 23(c)(4).

108. No unusual difficulties are likely to be encountered in the management of this action as a class action.

CLAIMS FOR RELIEF

COUNT I – NEGLIGENCE
(On behalf of Plaintiff and the Class)
(Against All Defendants)

109. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 108.

110. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting Plaintiff's and Class Members' information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things:

i. designing, maintaining, and testing Defendants' security protocols to ensure that the private information of Plaintiff and the Nationwide Class in Defendants' possession was adequately secured and protected;

j. to use reasonable care in obtaining, maintaining, and securing private information in Defendants' possession;

k. to impose processes to aptly discover and prevent the improper access and misuse of the personal information of Plaintiff and the Nationwide Class;

l. to adequately disclose that the personal information of Plaintiff and the Nationwide Class within Defendants' possession might have been compromised, how it was compromised, and the types of data that were compromised and when.

111. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly considering Defendants' insufficient security practices.

112. Defendants' own conduct created foreseeable risks of harm to Plaintiff and the Nationwide Class. Defendants' misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included its decisions not to comply with industry standards for the safekeeping of the personal information of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendants.

113. Plaintiff and the Nationwide Class had no ability to protect their personal

information that was in, and possibly remains in, Defendants' possession.

114. Defendants were in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

115. Through their actions and/or omissions, Defendants unlawfully breached their duties to Plaintiff and the prospective Class Members by

a. failing to design, maintain, and test their security protocols to ensure that Plaintiff's and the prospective Class Members' private information was adequately secured;

failing to use reasonable care in obtaining, maintaining, and securing private information in Defendants' possession;

b. failing to implement processes to rapidly discovery and preclude the improper access and misuse of personal information of Plaintiff and the Nationwide Class; and

c. failing to adequately disclose that Plaintiff's and the prospective Class Members' personal information might have been compromised, how it was compromised, and the types of data that were compromised and when.

116. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, their personal information would not have been compromised.

117. There is a close causal connection between Defendants' failure to implement security measures to protect the personal information of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The personal information of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of

Defendants' failure to exercise reasonable care in safeguarding such personal information by adopting, implementing, and maintaining appropriate security measures.

118. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect personal information. The FTC's publications and orders described above also form part of the basis of Defendants' duty in this regard.

119. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of personal information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

120. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

121. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

122. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class.

123. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the loss of the opportunity of how their personal information is used;

c. the compromise, publication, and/or theft of their personal information;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their personal information;

e. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

f. costs associated with placing freezes on credit reports;

g. the continued risk to their personal information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information of Plaintiff and the Nationwide Class; and

h. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the personal information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

124. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

125. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer the continued

risks of exposure of their personal information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in its continued possession.

126. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT II – BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)
(Against Defendants FNF and LoanCare)

127. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 108.

128. Through their course of conduct, Defendants FNF and LoanCare, Plaintiff, and Class Members entered into implied contracts for the provision of services for virtualization and cloud computing and/or other services, as well as implied contracts for Defendants to provide mortgage, loan, cloud computing/virtualization, and/or networking services, and implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

129. The valid and enforceable implied contracts for services that Plaintiff and Class Members entered into with Defendants include the promise to protect non-public PII given to Defendants or that Defendants create on their own from disclosure.

130. When Plaintiff and Class Members provided their PII to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

131. Defendants solicited and invited Class Members to provide their PII as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their PII to Defendants.

132. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

133. Class Members who paid money to Defendants reasonably believed and expected that Defendants would use part of those funds to ensure adequate data security. Defendants failed to do so.

134. Under the implied contracts, Defendants promised and were obligated to: (a) provide services to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their PII.

135. Both the provision of services and the protection of Plaintiff's and Class Members' PII were material aspects of these implied contracts.

136. Upon information and belief, the implied contracts for the provision of services that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendants' privacy notices.

137. Defendants' express representations, including, but not limited to the express representations found in their privacy notices, memorialize and embody the implied contractual obligation requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

138. Defendants' consumers value their privacy, the privacy of their dependents, and the ability to keep their PII associated with obtaining services private. To customers such as Plaintiff and Class Members, services that do not adhere to industry standard data security protocols to protect PII are fundamentally less useful and less valuable than services that adhere to industry-standard data security. Plaintiff and Class Members would not have entrusted their PII to Defendants and entered into these implied contracts with Defendants without an understanding that their PII would be safeguarded and protected or entrusted their PII to Defendants in the absence of Defendants' implied promise to adopt reasonable data security measures.

139. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their PII to Defendants, and paid for the provided services in exchange for, amongst other things, both the provision such services and the protection of their PII.

140. Plaintiff and Class Members performed their obligations under the contract when they paid for their services and provided their PII.

141. Defendants materially breached their contractual obligations to protect the non-public PII Defendants gathered when the sensitive information was accessed by unauthorized personnel as part of the Data Breach.

142. Defendants materially breached the terms of the implied contracts. Defendants did not maintain the privacy of Plaintiff's and Class Members' PII as evidenced by their late notifications of the Data Breach to Plaintiff and at least 1.31 million Class Members. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' PII, as set forth above.

143. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

144. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

145. Had Defendants disclosed that they did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased services from Defendants.

146. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their PII, the loss of control of their PII, the imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

147. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

148. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity monitoring to all Class Members.

COUNT III – UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

(Against Defendants FNF and LoanCare)

149. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 108.

150. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they provided their private information to Defendants in exchange for Defendants' goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

151. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

152. The amount Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendants' network and the administrative costs of data management and security.

153. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

154. Defendants failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

155. Defendants acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

156. If Plaintiff and Class Members knew that Defendants had not reasonably secured their PII, they would not have agreed to Defendants' services.

157. Plaintiff and Class Members have no adequate remedy at law.

158. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

159. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

160. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

COUNT IV – DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Class)
(Against All Defendants)

161. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 108.

162. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court may enter a judgment declaring the rights and legal relations of the Parties and grant further necessary relief. The Court also has broad authority to restrict acts that are tortious and violate the terms of regulations described in this Complaint.

163. There is an actual, substantial controversy concerning Defendants' present and prospective obligations to reasonably protect consumers' private information and whether Defendants are upholding cybersecurity measures sufficient to protect the Class, including Plaintiff, from future security breaches that risk Plaintiff's and Class Member's information.

164. Plaintiff avers that Defendants' cybersecurity measures are insufficient. Also, Plaintiff and Class Members still suffer injury from the Data Breach and stay at imminent risk that future breaches of their private information and ongoing fraud against them will happen.

165. Plaintiff petitions the Court to enter a judgment declaring the following: (i) Defendants owe a duty to protect consumers' private information and to timely notify them of a data breach under common law and Section 5 of the FTC Act; and (ii) Defendants are in in violation of these legal duties by failing to impose reasonable measures to protect consumers' private information in their possession and control.

166. Plaintiff asks the Court to issue injunctive relief mandating Defendants to use appropriate security controls consistent with law and industry standards to safeguard consumers' private information from future data breaches.

167. If an injunction is not issued, the Class Members will suffer irreparable injury and lack a sufficient legal remedy, should another data breach involving Defendants occur. The risk of

another breach is real, immediate and substantial. If another breach involving Defendants happens, the Class Members will not have an adequate legal remedy because several of the corresponding injuries are not readily quantified and Class Members will be compelled to bring several lawsuits to correct the same misconduct.

168. The hardship to Class Members if an injunction is not granted exceeds the hardship to Defendants if an injunction is granted. If a similar security breach happens again from Defendants' repeated misconduct, Class Members likely will be subjected to substantial hacking attempts and other damage. The cost to Defendants of complying with an injunction by imposing reasonable cybersecurity standards is minimal, and Defendants have pre-existing legal duties to impose such measures.

169. Issuance of the petitioned injunction will not harm the public interest. Rather, such an injunction would behoove the public by precluding further data breaches involving Defendants, thereby eliminating the additional injuries that would result to the Class Members and the millions of consumers whose private information would be further at risk.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: January 8, 2024

Respectfully submitted,

/s/ Francesca Kester Burne

Antonio Arzola, Jr.
FL Bar No 1040686.
Francesca Kester Burne
FL Bar No. 1021991
MORGAN & MORGAN
COMPLEX LITIGATION GROUP.
201 N. Franklin Street
Tampa, Florida 33602